

REMARKS

Reconsideration and allowance of this application are respectfully requested. Claim 7 is cancelled, and claims 12-13 are added. Claims 1-6 and 8-11 remain in this application as amended herein. Accordingly, claims 1-6 and 8-13 are submitted for the Examiner's reconsideration.

The specification has been amended to conform with the steps shown in Fig. 5. No new matter has been added by these changes.

In the Office Action, the Examiner rejected claims 1-11 under 35 U.S.C. § 103(a) as being unpatentable over Yoshiura (U.S. Patent No. 6,131,162) in view of Iida (U.S. Patent No. 6,209,787). Claim 7 has been cancelled. It submitted that the remaining claims are patentably distinguishable over the references.

The Yoshiura patent describes the distribution of content from a provider system to a purchaser system and the subsequent identification of purchasers that have illegally copied the content. The purchaser system generates a signature key and a verification key, stores the signature key, and sends the verification key to the provider system. The provider system then encrypts the stored content using the verification key and sends the encrypted content to the purchaser system. The purchaser system next decrypts the encrypted content using the stored signature key, generates a digital signature of the decrypted content using the signature key, and embeds the digital signature into the decrypted content. The embedded digital signature cannot be removed. If the purchaser illegally copies the content and the illegally copied content is subsequently seized and stored in the provider system, the provider system may extract the digital signature from the content and identify the purchaser who made the illegal copy by comparing the extracted digital signature with a hash value

associated with the purchaser. (See Figs. 2, 5 and 6; and col. 13, line 1 - col. 2, line 34).

Yoshiura therefore uses the digital signature to *identify illegal copiers* of the content. The patent does not disclose or suggest an apparatus having a unit that receives authentication information from another apparatus *when the another apparatus requests permission* to receive the encrypted content.

Moreover, though Yoshiura describes sending a verification key, the verification key is sent *from the purchaser system to the provider system*, is sent *before* the extracted digital signature is compared with the hash value associated with the purchaser, and is *encrypted* at the provider system with the content. Further, though the encrypted content (which includes the verification key) is then sent from the provider system to the purchaser system, the verification key is *not used to decrypt* the encrypted content. Rather, the purchaser system decrypts the encrypted content using the signature key. The patent does not disclose or suggest an apparatus having a unit that transmits a decryption key to another apparatus when authentication information is valid, and the patent does not disclose or suggest that the transmitted decryption key is needed to decrypt the encrypted content.

The Iida patent relates to a system that allows for the selection of musical compositions, the editing of the selection of musical compositions and related information, the storing of the edited musical compositions and related information in a recording medium, and the purchase of the recording medium. (See Abstract, and col. 1, lines 10-16). The Iida patent does not remedy the above-described deficiencies of Yoshiura.

Therefore, neither Yoshiura nor Iida suggests:

an authentication unit operable to receive authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content and to determine whether the authentication information is valid;

and neither reference suggests:

a transmitting unit operable to transmit a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content

as called for in claim 1.

It follows that neither Yoshiura nor Iida, whether taken alone or in combination, discloses or suggests the information processing apparatus defined in claim 1, and claim 1 is therefore patentably distinct and unobvious over the references.

Claims 2-3 depend from claim 1, and each claim further defines and limits the invention set out in the independent claim. It follows each of claims 2-3 likewise defines a combination that is patentably distinguishable over the references.

Independent claim 4 relates to a method for carrying out secure transmission of content from an information processing apparatus to another apparatus over a network. The claim calls for:

receiving authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content;

and further calls for:

transmitting a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content[.]

Therefore, claim 4 is patentably distinguishable over Yoshiura and Iida for at least the same reasons.

Independent claim 5 relates to a recording medium having recorded thereon a program for executing the method recited in claim 4. Claim 5 is therefore patenably distinguishable over the references at least for the same reasons.

Independent claim 6 defines an information processing apparatus that includes a second authentication unit and a first obtaining unit having limitations similar to those set out in claim 1. Claim 6 is therefore patentably distinguishable over Yoshiura and Iida for at least the same reasons.

Claims 8-9 depend from claim 6 and are also distinguishable over the references for at least the same reasons.

Independent claim 10 is directed to a method for carrying out secure receiving of content from a first apparatus over a first network and for carrying out secure transmission of a content to a second apparatus over a second network. Claim 10 includes steps having limitations similar to those set out in claim 4. Therefore, claim 10 is patentably distinguishable over Yoshiura and Iida at least for the same reasons.

Independent claim 11 relates to a recording medium having recorded thereon a program for executing the method defined in claim 10. Claim 11 is therefore distinguishable over the cited art for at least the same reasons.

Accordingly, the withdrawal of the rejection under U.S.C. § 103(a) is respectfully requested.

New claim 12 depends from claim 1, and new claim 13 depends from claim 6. Therefore, each of new claims 12 and 13 is distinguishable over the cited references for at least the same reasons. Support for these claims is found, e.g., in Figs. 5-10 and in paragraphs [0048]-[0074] of the specification.

As it is believed that all of the rejections set forth in the Official Action have been fully met, favorable

reconsideration and allowance are earnestly solicited. If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that the Examiner telephone applicant's attorney at (908) 654-5000 in order to overcome any additional objections which the Examiner might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: April 28, 2005

Respectfully submitted,

By 

Lawrence E. Russ

Registration No.: 35,342

LERNER, DAVID, LITTENBERG,

KRUMHOLZ & MENTLIK, LLP

600 South Avenue West

Westfield, New Jersey 07090

(908) 654-5000

Attorney for Applicant

553494_1